Requested Patent: JP7084852A

Title: SECURITY SYSTEM FOR INFORMATION ;

Abstracted Patent: JP7084852 ;

Publication Date: 1995-03-31 ;

Inventor(s): TANAKA KAZUAKI; others: 02 ;

Applicant(s): HITACHI LTD ;

Application Number: JP19930225440 19930910 ;

Priority Number(s): ;

IPC Classification: G06F12/00; G06F3/14; G06F12/14 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To offer information to limited users and to restrict the takeout of a copy of the information and also prevent it by providing a program, which controls a read of displayed screen data, with a function which limits the read.

CONSTITUTION:This system is provided with a database server 1, a client work station 2, and a network 3, and the window server 22 of the client work station 2 performs an input/output process on a display screen at a request made by a user interface program 13 in the server 1. Then a document management file while managing a document file itself wherein substance data on a document are stored manages whether the document can be referred to or copied. At this time, a reference management program checks a reference right management file for a document file whose reference management attribute indicates 'limited' to check whether or not a referring person has the right to refer or copy, thereby deciding whether the the person is allowed to refer to or copy the document file.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平7－84852

(43)公開日　平成７年(1995)３月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	12/00	５３７　Ｍ	8944－5Ｂ		
	3/14	３４０　Ａ			
	12/14	３２０　Ａ			

審査請求　未請求　請求項の数９　ＯＬ　（全７頁）

(21)出願番号　特願平5－225440

(22)出願日　平成５年(1993)９月10日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　田中　和明
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　能見　誠
茨城県勝田市市毛1070番地　株式会社日立製作所水戸工場内

(72)発明者　岩崎　一正
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

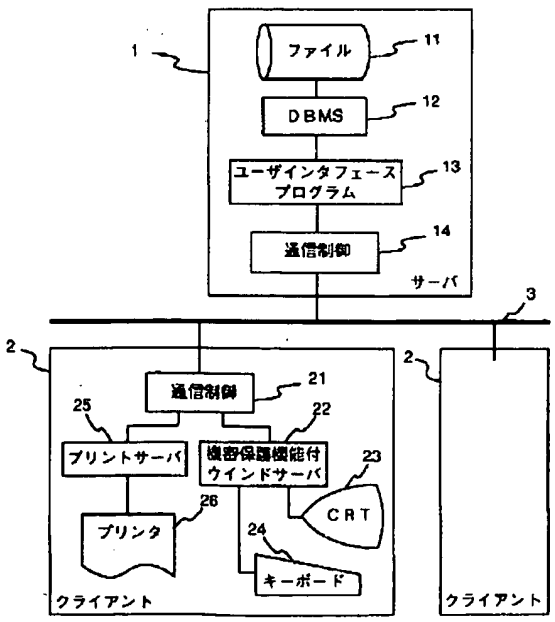
(54)【発明の名称】　情報の機密保護方式

(57)【要約】

【構成】データベースサーバ１，クライアントワークステーション等により構成し、ファイル参照管理で参照の可否，複写の可否を管理し、特に複写の可否によって他の媒体への複写を禁止する機能を備え、更に、画面表示を司るウインドサーバ２２に画面のハードコピーを制限する機能を設けた。

【効果】限られた範囲のユーザにデータベースの情報を提供し、かつ、その情報の複写持出しを制限，防止する上に大きな効果がある。

図1



1

【特許請求の範囲】

【請求項１】文書，データのファイルを蓄積し、それを利用する計算機システムにおいて、ファイルの参照と共に複写の可否を登録し、その可否によって参照，複写を制限することを特徴とする情報の機密保護方式。

【請求項２】請求項１において、情報を表示する端末の表示制御機能に表示画面の読みだしを制限する機能を付加することによって表示画面のハードコピーを制限する情報の機密保護方式。

【請求項３】請求項１において、情報の複写媒体ごとに複写の可否を制限する機能を備えた情報の機密保護方式。

【請求項４】請求項１において、複写の可否を参照者もしくは参照者グループ対応に登録し、その登録情報に基づいて複写を制限する情報の機密保護方式。

【請求項５】請求項１において、複写の可否を情報種別対応に登録し、その登録情報に基づいて複写を制限する情報の機密保護方式。

【請求項６】請求項２において、マルチウインドを表示する機能を備えた端末を具備し、前記端末においてウインド毎に読みだし可否の属性を管理する機能を備え、少なくも一つの読みだし禁止ウインドを表示している間は画面の表示データを読みだすことを禁止する機能を備えた情報の機密保護方式。

【請求項７】請求項６において、情報を送り出すプログラムより端末の表示ウインドに読みだし禁止属性を設定した後に、その読みだしを指示し、読みだしが不可能であれば禁止機能がはたらいていると判断して、複写禁止の対象となっている情報を表示する情報の機密保護方式。

【請求項８】請求項６において、情報を送り出す機能と表示する端末を一つの計算機で実現した情報の機密保護方式。

【請求項９】計算機のマルチウインドシステムのウインドサーバにおいて、各ウインド単位のウインド管理情報の中に複写可否を指定するための複写可否属性を付与し、ウインドサーバへの表示画面データ読みだし要求があったとき、表示中の全てのウインドの複写可否属性をチェックし、少なくも一つのウインドが複写可否属性が否を示す場合、画面表示データの読みだしを禁止する機能をこと備えたことをを特徴とするウインドサーバシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はコンピュータ上に蓄積され、端末等によってそのデータを参照する情報システムに係り、その参照，複写等の制限を設けて情報の保安を管理する方法に関する。

【０００２】

【従来の技術】従来、計算機上の情報の参照を制限する

2

最も単純な方法は、例えばワークステーションのオペレーティングシステム（以下ＯＳと略す）であるユニックス（Unix）の場合、利用者に識別コード、いわゆる、ＩＤコードを与え、かつ、そのＩＤコードに対応する個人のパスワードを与え、このパスワードを当人、あるいは特定のグループ以外に秘密とすることで，他人が管理する情報を許可無く参照することを禁止する方法がある。この方法では、このＩＤコード，パスワードの他に、プログラム，情報ファイルに参照権利属性を付与して書き込み，読みだしの権利を個人，グループ，その他の複数のレベルで管理できるようにしているのが一般的である。

【０００３】この方法の拡張として、更に、特定の情報、例えば、データベース等を限定的に参照許可を与える方法として、ファイルのアクセス権ではなく、データベースへの接続権を限定し、更に特定のＩＤとパスワードを与え、階層的な保護を図る方法が利用されている。

【０００４】一方、重要な情報の機密保護等を必要とする場合は、上記一般的な方法に加えて、参照の手続き、及び情報そのものを暗号化して特定の暗号化、復号機構を備えた端末等によりアクセスし、かつ暗号の鍵を特定者に与えることによってそれ以外の者が参照，解読，盗聴不可能なシステムが提供されている。

【０００５】一方、著作権に基づく不法なプログラム，データの複写を防止するためには、コピープロテクトのための情報を付加し、その格納された媒体上に参照プログラムを同居させ、その参照プログラムによって目的とするプログラム，データを参照するもので、その参照プログラム以外のＯＳ等では直接参照出来ないようにすることによってプロテクトを実現する方法が一般的である。

【０００６】

【発明が解決しようとする課題】以上のような保護方法を用い、汎用のUnixワークステーションあるいは汎用パーソナルコンピュータを用いて、例えば、企業内の情報システムを構築した場合、企業内の社員は自由、あるいは緩やかな制限で参照できる必要のある情報を扱った場合、参照そのものは問題無いが、それを物理的な媒体、例えばフロッピーディスクにコピーしたもの、あるいはプリントアウトした書類は外部には持ち出してはならない情報が存在する。製品の開発，設計，製造に関わる技術情報はその種の情報の一例である。

【０００７】このような情報は、他の媒体に複写，印刷するのを防止することは、それを参照するプログラムを専用のものにすることにより比較的容易に実現することが可能である。

【０００８】しかし、一般のワークステーション，パーソナルコンピュータは表示された画面をそのまま印刷する機能を持っているか、持っていなくても他のプログラムを動作させて表示されている画面を容易に印刷するこ

3

とが出来るようになっているため、自由に表示画面を印刷可能となり、一方、その画面印刷機能が無ければ通常の利用で不都合が生じることになり、その機能を無くすことは出来ないという問題がある。

【0009】

【課題を解決するための手段】以上の問題を解決するために、表示された画面データの読みだしを司るプログラムに読みだしを制限する機能を設け、かつ、読みだしを制限すべき情報の表示領域（ウインドー）に読みだし制限の属性を持たせることによって解決する。

【0010】

【作用】以上のような手段を設け、特定情報を表示するプログラムは上記読みだし制限の属性を表示ウインドーに与えて、表示し、一方、画面の読みだしを行うプログラムは読みだしを制限されたウインドーが少なくも一つ表示画面上に存在する場合は、その全面を読みだし禁止とするか、あるいは、読みだしを制限されたウインドーの領域のみ読みだし不可能として白地に抜いたデータを読みだし要求のあったプログラムに渡す等の手続きを実行することによって機密保護情報の印刷を防ぐことが出来る。

【0011】

【実施例】以下、本発明の実施例を図に従って説明する。

【0012】図1は本発明を実施する情報システム全体の構成例を示したもので、1は情報を蓄積し、要求に応じて情報を提供するデータベースサーバ、2はその情報を参照するためのクライアントワークステーション、3はネットワークである。

【0013】更に、データベースサーバ1の内部を機能的に表現したものとして、11はデータベースファイルであり文書等のデータ及びその管理情報が格納されている。12はデータベース管理システム（以下ＤＢＭＳ）、13はユーザインタフェースプログラム、14は通信制御機能である。

【0014】一方、クライアントワークステーション2の内部を機能的に表現したものとして、21はサーバ内の通信制御と対になってコマンド，データの授受を行うための通信制御機能である。22はウインドーサーバでUnixシステムのＸ－windowサーバ等がこれに相当し、サーバ1の中のユーザインタフェースプログラム13の要求に応じて表示画面上での入出力処理を行う。又、23はプリントサーバで13の要求に応じて文書や表示画面の印刷処理を行う。

【0015】このようなデータベースシステムにおいて、情報の機密管理は、通常計算機システムを利用する上でのＩＤ，パスワード管理と、データベースを利用する上でのＩＤ，パスワード管理が多重に行われ、情報の機密管理はＤＢＭＳ12又はユーザインタフェースプログラム13、あるいはその双方において後者を主体に行

4

われているが、参照の可否を管理しているに過ぎず、本発明では参照可否の他に参照結果の複写をも管理する。

【0016】図2はその複写管理方法の例を説明したもので、文書管理ファイルは文書の実体データの格納されている文書ファイル自身を管理すると同時に、その参照及び複写可否の管理を行う。

【0017】この時、参照管理プログラムはファイルの参照管理属性が「制限」を示している文書ファイルＷａの場合は、参照権管理ファイルをチェックして参照者が参照権，複写権を得ているかどうかをチェックしてその参照，複写を許可するかどうかを判定する。

【0018】図2の例の場合はＩＤが「ＮＮＮＮＮ」の参照者は参照権が「許可」であるが、複写権が「不許可」となっているため複写要求を出してもそれは受け付けられないのに対して、ＩＤが「ＭＭＭＭ」の参照者は複写権が「許可」と登録されているため、複写要求は受け付けられ、複写サービスを受けることが出来る。

【0019】一方、文書ファイルＦｂは参照管理属性がファイルそのものを複写不可とする「複写禁止」となっているため、参照者の権利のいかんに関わらず複写は許可されない。

【0020】他方、参照管理属性が「無制限」となっている文書ファイルＦｃとＦｄは参照のみならず複写の制限もなく、無条件に複写サービスを受けることが可能であることを示している。

【0021】このように、ファイルの参照，複写サービスを提供するか否かの管理を行うことが可能となる。

【0022】この場合、「複写」の持つ意味は、データとしてファイルをフロッピーディスク等の他のメディアや他のワークステーションの磁気ディスク等の外部記憶装置への複写のみならず、プリンタへの出力も含まれるが、何に複写するかまでも細かく管理したい場合は、複写権管理ファイルの管理項目をきめ細かくすることによって可能である。

【0023】しかし、以上のような管理を行っても、Unix等のＯＳ，Ｘ－windowのウインドサーバを搭載したワークステーションシステムの場合は、全く異なるプログラムを並行して動作させ、かつ、同一のディスプレイにマルチウインドで複数の画面を同時に表示することが出来、複写禁止の文書を一つのウインドで表示し、それとは関係のないプログラムを動かし今一つのウインドを表示し、そこから表示画面のハードコピーをウインドサーバ，プリントサーバを経由して複写禁止の画面をコピーすることは可能で、従来のウインドサーバ，プリントサーバをそのまま利用する限りこれを防止することは出来ない。

【0024】それを示したのが図3で、ウインドＷａは複写禁止の文書を表示しており、他方、ウインドＷｂ，Ｗｃ，Ｗｄは複写を禁止されていない情報を表示している場合を示したもので、例えば、ウインドＷｂより画面

5

のハードコピーを要求するプログラムを動かせば、複写禁止ウインドを含めて画面全体をプリントアウトすることが出来る。

【００２５】もちろん、ウインドＷａを全面に表示し、ウインドＷｂを一時消去して、複写禁止文書の画面のみをプリントアウトすることも可能である。

【００２６】そこで本発明は更に、画面（ウインド）を表示する時に、ウインドの属性として複写管理属性を持たせ、それが「複写禁止」となっているウインドが表示されている場合は、表示画面の読み取り，複写を禁止する機構を設けてそれを防止するものである。

【００２７】図４はその属性を付加したウインド管理テーブルの一例を示したもので、一つのウインド管理テーブルには複写権の有無を設定する項目を追加し、既にある表示状態管理情報とを用いてその管理制御を行う。

【００２８】図４で示す例は、ウインドＷａが複写禁止属性を持ち、他のウインドＷｂ，Ｗｃ，Ｗｄは複写禁止となっていない。

【００２９】従って、この場合は、ウインドＷａが画面上に表示されている限りは他のウインドから画面コピーを要求しても、ウインドを管理しているウインドサーバが画面データを渡さないようにしておけば以上の問題を解決することが出来る。

【００３０】図５は、参照者の要求に基づいて例えば文書ファイルを検索し、それを表示するユーザインタフェースプログラムのフローチャートの一例を示したもので、ステップ３０１，３０２は参照権チェックのためのユーザＩＤ，パスワードの入力である。この場合、ユーザＩＤ、及びパスワードの入力はワークステーションを利用開始時に入力するものをそのまま使用しても良いし、管理を厳しくするために別に設けても良い。又、ステップ３０１，３０２でユーザＩＤ、及びパスワードの入力だけではなく、このデータベースシステムのサービスを提供すべきユーザであるかどうかをチェックしてもよい。

【００３１】次に３０３で検索項目を入力し、それに基づいてステップ３０４でデータベースに登録されたファイルを検索し、該当なファイルが存在しない場合は終了とし、ファイルがあった場合は次のステップ３０６，３０７で参照権，複写権のチェックを行う。

【００３２】この時のチェックは図２に示す文書管理ファイル，参照管理ファイルのデータに基づいて行う。

【００３３】ここで一般のデータベースと同様に、ユーザに参照権が与えられていない場合は、ここでは省略しているが、許可されていないことをユーザにメッセージを出して終了する。

【００３４】一方、参照権が与えられている場合は、更にステップ３０７で複写権が与えられているかチェックし、複写権が与えられている場合はステップ３１０で複写許可の属性を持つウインドを生成し、他方、複写権の

6

無い場合はステップ３０９でウインドサーバが画面読み出しを禁止出来ているかどうかを確認し、読み出し可能であれば禁止機能がないとして表示を打切り、禁止出来ていれば読みだし保護が可能であると判断してステップ３１１以降の処理に入る。

【００３５】そのあとでステップ３１１でファイルを読みだし、ステップ３１２でその表示データをクライアントワークステーション２のウインドサーバに送信することでユーザが利用しているワークステーションの表示画面上に文書ファイルが図３の例のように表示されることになる。

【００３６】次に、図６はこの画面のハードコピーを他のプログラム等からプリントサーバに要求したときのプリントサーバのハードコピープログラムの一例を示したもので、印刷要求によって処理を開始し、ステップ４０１で表示画面の読みだし受渡しをウインドサーバに要求し、ステップ４０２でリターン情報でそれが正常に受け渡されたか、あるいは、複写禁止ウインドが含まれているかをチェックし、禁止されていなければ、ステップ４０３でその画面データをプリンタへ送り、ステップ４０４で印刷完了を待って終了する。

【００３７】一方、画面の表示データを要求されたウインドサーバは、図７の例に示すように、ステップ５０１でウインド管理テーブルをチェックし、複写禁止属性を持つウインドが表示されていないときのみステップ５０２で画面データを読みだし、ステップ５０３で要求元にそのでデータを受け渡す。

【００３８】以上のように、ウインドサーバが表示画面データの読みだしをウインド管理情報の複写権属性と表示状態を監視し、その読みだし可否によって受渡しを管理制御出来るようにすることによって表示画面の複写を制限する機能を実現することが可能となる。

【００３９】次に、図８は文書ファイルをデータベースに登録する際の参照管理を行うときの処理を示したもので、ステップ６０１で参照属性を入力し、ステップ６０２でその属性を判断し、参照が禁止の場合はステップ６０３で参照禁止属性を付与し、参照制限であればステップ６０４で参照制限属性を付与し、ステップ６０５でその参照を管理するための参照管理ファイルを生成する。無制限であればステップ６０６で参照無制限属性を付与して、ステップ６０７でファイルを格納する。

【００４０】この場合、基本の管理は参照のみとしそのもとで複写の可否を制限したものを示したが、情報の性格から無条件に複写が禁止されるべきものもあり、この場合は属性情報に複写禁止属性を追加すればその管理を行うことが出来る。

【００４１】更にユーザごとの参照権登録処理のフローチャートとを示したものが図９である。図９において、データベース管理者は登録対象者と参照対象文書ファイルを指定し、システムはステップ７０１，７０２でそれ

7

を入力する。次にそれに対応した参照権をステップ７０３で入力し、ステップ７０４でそれをチェックし、参照権が与えられている場合はステップ７０５で参照許可属性を設定し、不許可であればステップ７０９で不許可属性を設定する。

【００４２】更に、参照権が与えられている場合は複写権をチェックし、複写権を与えている場合はステップ７０７で複写許可を設定し、与えない場合は不許可を設定する。その結果をステップ７１０で参照管理ファイルに登録して終了する。

【００４３】尚、図９では文書，参照者毎に参照権の設定を行っているが、文書の種類，参照者グループ毎の単位で設定，管理を行っても良い。

【００４４】

【発明の効果】本発明によれば、限られた範囲のユーザにデータベースの情報を提供し、かつ、その情報の複写持出しを制限，防止する上で大きな効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例のブロック図。

【図２】本発明の文書管理ファイルの実施例の説明図。

【図３】本発明の画面表示例の説明図。

8

【図４】本発明のウインド管理テーブルの実施例の説明図。

【図５】本発明のデータベース検索処理実施例のフローチャート。

【図６】本発明の一実施例の画面印刷プログラムのフローチャート。

【図７】本発明の一実施例のウインドサーバの画面読み出し機能のフローチャート。

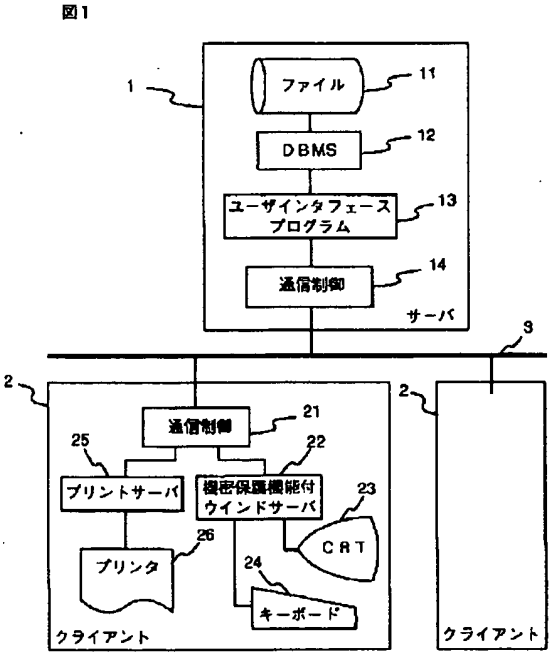
【図８】本発明の一実施例のデータベース参照，複写管理属性設定処理のフローチャート。

【図９】本発明の一実施例の参照者単位の参照権，複写権登録プログラムのフローチャート。

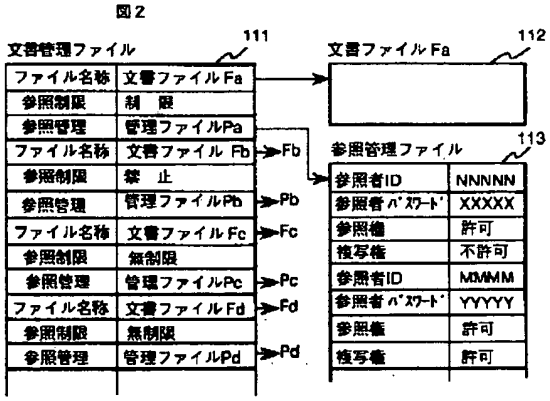
【符号の説明】

１…データベースサーバ、１１…その中のファイルシステム、１２…データベース管理システム、１３…ユーザインタフェースプログラム、１４…通信制御機能、２…クライアントシステム、２１…通信制御機能、２２…機密保護付きウインドサーバ、２３…ディスプレイ装置、２４…キーボード、２５…プリントサーバ、２６…プリンタ、３…サーバとクライアントを結ぶネットワーク。

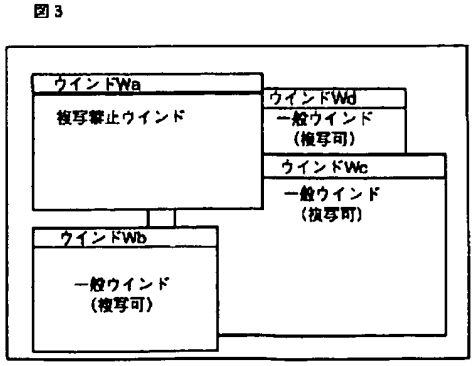
【図１】



【図２】

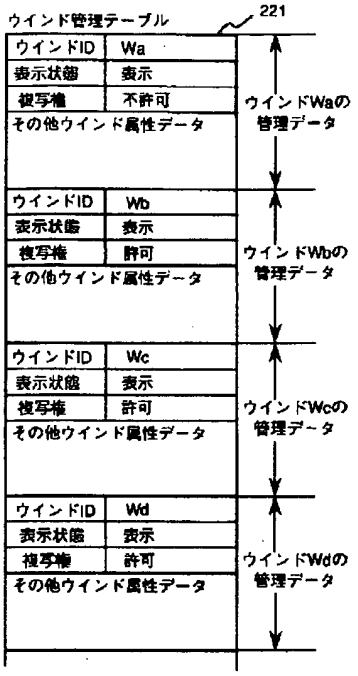


【図３】



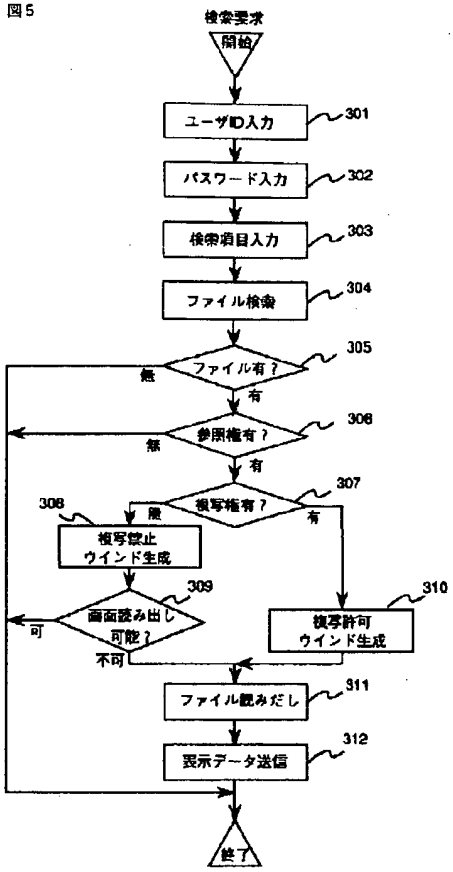
【図4】

図4



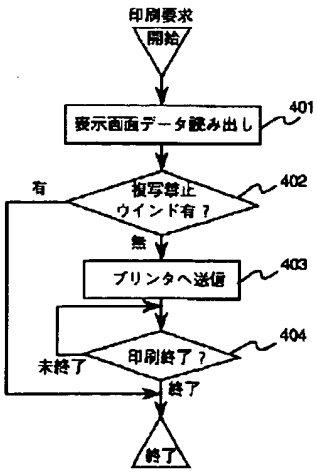
【図5】

図5



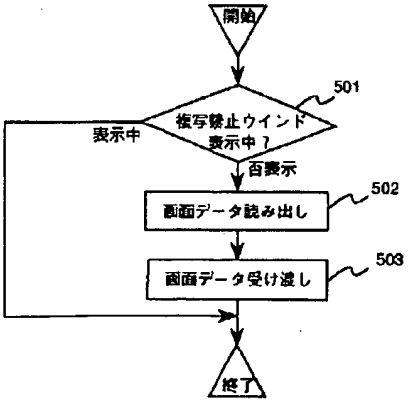
【図6】

図6



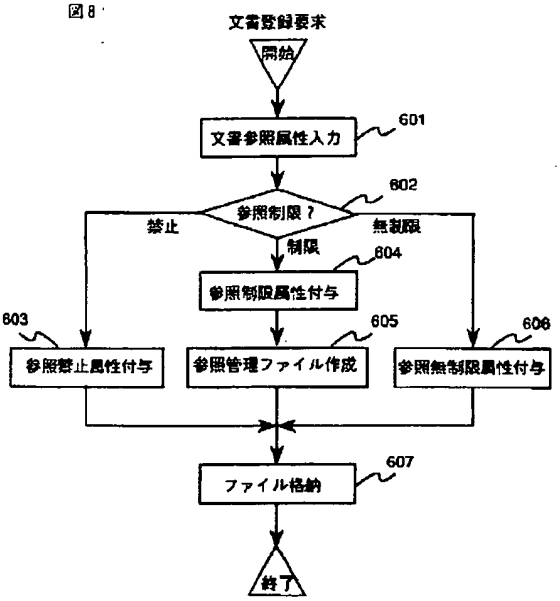
【図7】

図7



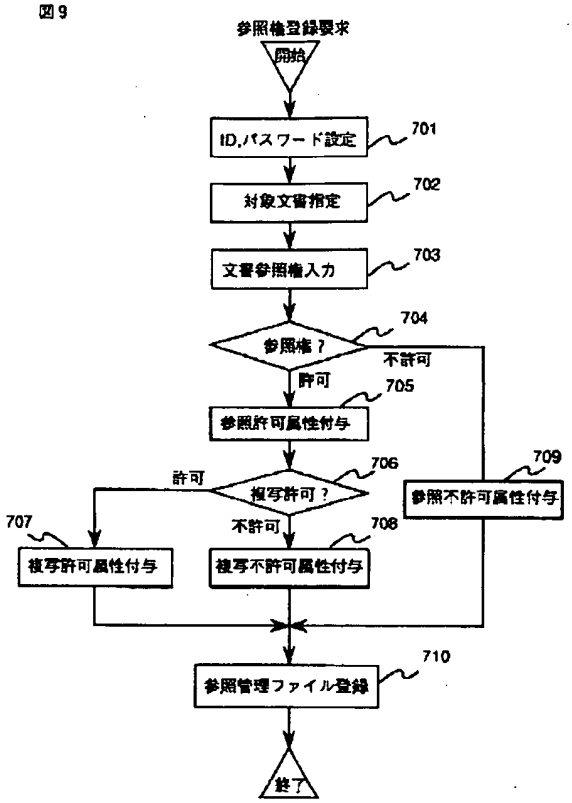
【図8】

図8


文書登録要求
開始
文書参照属性入力
601
参照制限？
602
禁止
制限
無制限
参照制限属性付与
604
603
参照禁止属性付与
参照管理ファイル作成
605
606
参照無制限属性付与
ファイル格納
607
終了

【図9】

図9


参照権登録要求
開始
ID,パスワード設定
701
対象文書指定
702
文書参照権入力
703
参照権？
704
不許可
許可
参照許可属性付与
705
許可
複写許可？
706
709
参照不許可属性付与
707
不許可
708
複写許可属性付与
複写不許可属性付与
参照管理ファイル登録
710
終了